Issue Brief: Federal Cloud Infrastructure Survey Results Summary

The Advanced Technology Academic Research Center (ATARC), in partnership with Rackspace, VMware, Amazon Web Services, and Carahsoft, recently conducted a survey aimed at understanding the current status of, and barriers to, the adoption of cloud services in the federal IT space. Participants were asked a series of questions regarding their views and assessments of their agencies' cloud implementation experience. The survey was conducted from April 5-23, 2021 and included over 100 participants representing 36 federal agencies ranging in seniority from executives to individual contributors.

Survey respondents painted a picture of a federal IT landscape that has made substantial progress in its cloud journey but where the challenges associated with multicloud management, understanding security and compliance requirements, and achieving FedRAMP ATO for cloud services continues to form a significant barrier.

Understanding the Lay of the Land

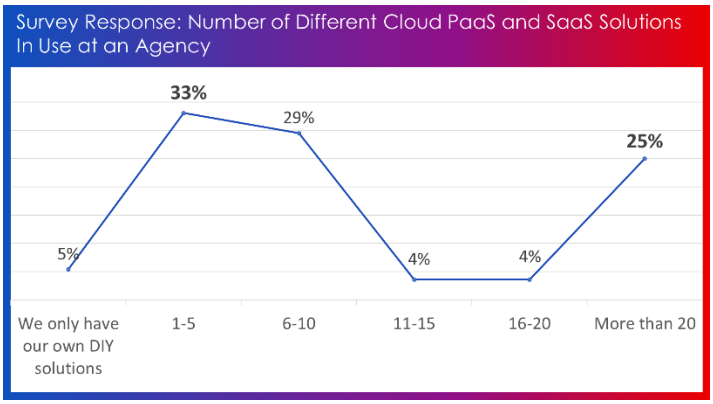
According to Jeff DeVerter, Chief Technology Officer, Products & Services at Rackspace, a multicloud strategy offers several benefits to organizations. Among the most important is the ability for organizations to "better match consumption with demand and increase their options for right-sizing resources." DeVerter adds that a multicloud approach enables "further opportunities for cost savings...from the reduction of cloud vendor lock-in and increased leverage in price negotiations."

A promising **37%** of respondents report their Agency to be using **multiple cloud solutions** and vendors, while another **60%** have at least **started on a cloud strategy journey**.

View Survey Results HERE

Federal agencies are clearly taking DeVerter's advice to heart, with 37% of survey respondents reporting that their agency is already using multiple cloud solutions and vendors to "optimize migration, security, and compliance," a trend that is only likely to continue. In fact, when asked about the future, respondents anticipated relying less on just private or public clouds, envisioning a scenario that more heavily leverages hybrid and multicloud models.

In line with the broader cloud market, Amazon Web Services and Microsoft Azure were the vendor cloud solutions respondents indicated to be most commonly deployed within their agencies. However, they are far from the only solutions being deployed. To illustrate, 33% of respondents said their agencies were already using one to five PaaS or SaaS solutions, 29% said they were using six to ten solutions, and a quarter reported that their agencies were using a whopping twenty or more PaaS or SaaS solutions.



Even among respondents whose agencies aren't already using multiple cloud solutions, the vast majority indicated that they had at least begun evaluating cloud migration paths, with many already having begun to migrate some systems. Indeed, just 4% of respondents said they hadn't shifted their cloud strategies at all. Respondents were also remarkably uniform when asked about the highest impact level technologies used by their agencies, with FedRAMP Moderate and FedRAMP High by far the most common at 43% and 32%, respectively.

Anticipating the Pitfalls

As might be expected given the level of effort their agencies are making to migrate on-premise systems to the cloud, survey respondents were clear about the benefits they anticipated to receive from the move. The most commonly cited of these benefits were increased business agility, the modernization of legacy systems, and the ability to provide an improved customer/citizen experience. The final benefit being of particular value to agencies looking to up-level their digital experiences in line with the 21st Century Integrated Digital Experience Act. However, barriers clearly remain.

With 26% ranking them at number one, budget constraints were the clear "leader" among the barriers cited by survey respondents as inhibiting the move from historically on-premise DIY solutions to best-of-breed vendor-provided cloud solutions. Other commonly cited barriers were the difficulty of hiring and retaining a workforce with the necessary skills to leverage vendor-provided cloud solutions and procurement challenges.

At any large organization, but especially one whose work involves sensitive employee and citizen data like a government agency, security is intimately tied to the procurement process. A cloud service must be thoroughly vetted for vulnerabilities and access controls before it is authorized for use. Unfortunately, this process can cause confusion and frustration for federal employees who are simply trying to procure the tools necessary to accomplish their mission objectives. This confusion was acutely felt by survey respondents, only 40% of whom indicated that they had a "strong" understanding of their agencies' security and compliance requirements.

79% of respondents agree with the notion that
FedRAMP helps ensure cloud security.

41% agree that FedRAMP hinders modernization through a slow ATO process.

View Survey Results HERE

One of the most important programs for ensuring that cloud services meet federal security and compliance procedures is the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP emerged in the early 2010s in order to establish a uniform assessment process for cloud services and has proven particularly useful for smaller agencies that might not otherwise have the resources to conduct full security audits on their own. Survey respondents were clear in articulating the benefits of FedRAMP, with 79% agreeing or strongly agreeing with the notion that FedRAMP "helps ensure cloud security." 62% of respondents also agreed or strongly agreed with the idea that FedRAMP streamlines the procurement of trusted cloud solutions.

However, FedRAMP is not without its limitations. In particular, the program is able to work with only a small number of cloud service providers (CSPs) every year and the costs associated with achieving Authority to Operate (ATO) through FedRAMP can be prohibitive for smaller vendors. The end result is that federal agencies have more limited choice in CSPs than their counterparts in the private sector. In fact, 29% of survey respondents agreed or strongly agreed with the notion that "FedRAMP is unintentionally forcing agencies towards shadow IT procurements," with an additional 40% of respondents unsure. 41% of respondents also agreed or strongly agreed with the idea that FedRAMP hinders modernization through a slow ATO process that results in fewer approved cloud solutions. In short, while the benefits of FedRAMP in standardizing the procurement of cloud services and ensuring security are clear, agencies need to be aware of the limitations in the ATO process.

Overcoming the Barriers

By 2022, over 90% of global enterprises will rely on a mix of on-premises/dedicated private clouds, multiple public clouds, and legacy platforms, IDC reports, marking 2021 as **the year of multicloud**.

It is important to note that the steady shift to embrace cloud modernization is rapidly accelerating with government increasing funding for cloud initiatives after the cloud proved invaluable in keeping agencies and critical response resources operational during the pandemic. Additionally, the cloud is considered the key by government security leaders in shifting from a defensive cyber posture to an offensive one.

Companies like Rackspace Government Solutions, VMware, AWS, and Carahsoft are working together to provide solutions and services that enable agencies to modernize and fully leverage and optimize their public and private cloud investments to ensure success across every stage of the cloud journey – assess, design, build, migrate, and innovate.

For example, Secure Multicloud-as-a-Service (McaaS) is a comprehensive managed cloud security solution – available through Rackspace Government Solutions for VMware or AWS environments – that protects and prevents enterprise and customer data, assets and applications from advanced security threats and cyberattacks while complying with all relevant government regulations and guidance. It simplifies the complexities of multicloud and frees agencies to focus on the mission, while entrusting cloud operations and security to the experts.

MCaaS can shorten the path to the cloud, increasing productivity while reducing overall total cost of ownership. Additionally, agencies can optimize the benefits of the cloud and move more quickly to leverage automation, software-based analytics tools, and capabilities utilizing emerging technologies like artificial intelligence and machine learning.

The partners are also working together to help CSPs accelerate their journey to FedRAMP ATO and, in turn, accelerate the availability of innovative cloud solutions to government agencies. With Rackspace Government Cloud (RGC) on VMware and Rackspace Government Cloud (RGC) on AWS, CSPs inherit up to 80% of the solution's over 325 security controls. Doing so dramatically cuts down the time needed to obtain FedRAMP authorization from years to as little as four months. RGC on VMware and RGC on AWS customers never have to start from scratch, they're able to build on existing investments to get to market faster and at lower cost.

The complexity that comes along with multicloud can be overcome with the right partners and resources. The key is a fully baked multicloud strategy with the right industry partners and a secure multicloud-as-a-service (McaaS) approach that streamlines and optimizes planning and unifies governance, security, and management across all cloud environments.